コンテンツ保護技術

コンテンツ配信技術11

菊池　浩明

プロテクト破り DeCSS

- CSS (Contents _____System)
  - 松下＆東芝の提案したDVD暗号化方式
  - 40bit共通鍵暗号（マスタ鍵，ディスク鍵，タイトル鍵）
  - 1999 ノルウェイの高校生(Jon Johansen)が公開

```
void CSSdescramble(unsigned char
*sec,unsigned char *key) { unsigned int
t1,t2,t3,t4,t5,t6; unsigned char
*end=sec+0x800; t1=key[0]^sec[0x54]|
0x100; t2=key[1]^sec[0x55];
t3=(*((unsigned int *)(key
+2)))^(*((unsigned int *)(sec+0x56)));
t4=t3&7; t3=t3*2+8-t4; sec+=0x80;
t5=0; while(sec!=end)
{ t4=CSStab2[t2]^CSStab3[t1];
t2=t1>>1; t1=((t1&1)<<8)^t4;
t4=CSStab5[t4];
t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5
)&0xff; t3=(t3<<8)|t6; t6=CSStab4[t6];
t5+=t6+t4; *sec+
+=CSStab1[*sec]^(t5&0xff); t5>>=8; } }
```

http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/

DeCSS開発者

- Jon Lech Johansen
  - 15歳でdeCSSを開発
  - 2002年ノルウェー検察当局は著作権法違反として起訴
  - 2003年無罪判決
- なぜか罪を問われなかったのか？

http://nanocr.eu/

著作権保護法

- 知的財産権
  - 工業所有権（特許，実用新案）
  - 著作権（文化的な著作物）
- 著作権
  - 著作物：論文，小説，楽曲，歌詞，絵画，地図，写真，映画，＿＿＿＿＿＿，プログラム，
  - 登録不要（著作物を創作したら権利発生），
  - 著作者の死後50年まで保護
- 著作者の権利
  - 著作者人格権：　公表権，同一性保持権
  - 著作権（財産権）：　＿＿＿＿権，上映権，公衆送信権，譲渡権

著作物を自由に使える例

＿＿＿＿のための複製	第30条	自分自身や家族など限られた範囲内で作る複製.
図書館などでの複製	第31条	図書館の利用者に対する複製
学校における複製	第35条	教育者と授業を受けるものは授業目的での複製. 試験問題(36条), 教科書(33条).
非営利目的の演奏会	第38条	料金を取らない上映, 演奏.

それって違法？

- Q1. 宿題にウェブサイトの文書や写真を無断
- Q2. 文化祭でゲームセンターを開いた.
- Q3. 教育目的で有料ソフトをコピーしてインストールした.
- Q4. アカデミック割引ソフトを卒業後も使った.
- Q5. 無料配布のパンフレットにキャラクター画像を使用.
- Q6. バンコクで極安ソフトウェアを購入した.

教育機関における複製

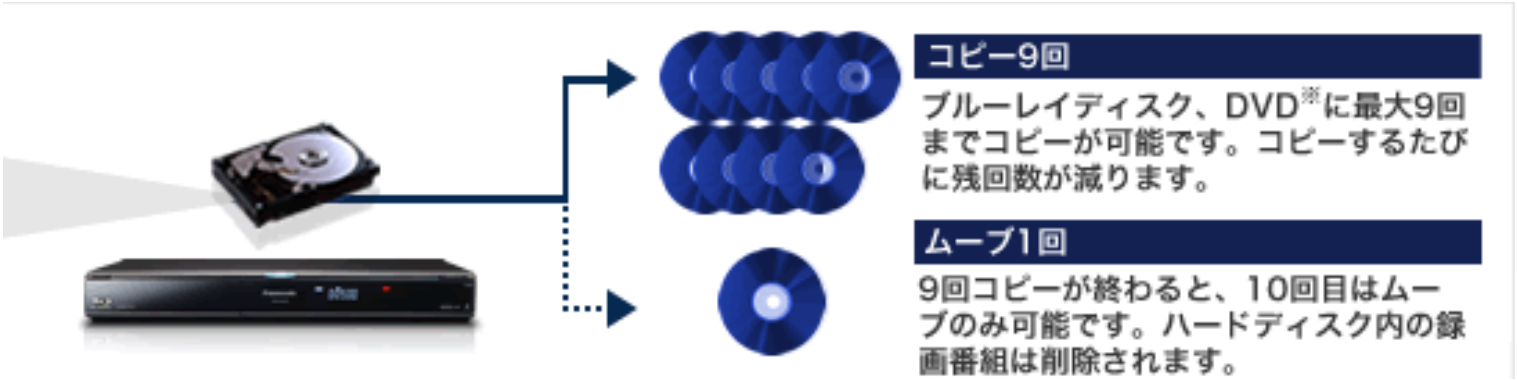
- 著作権法35条1項で規定される条件
  （1）営利を目的としない教育機関であること
  （2）教育を担当している教員等やその授業を受ける者が複製すること
  （3）公表された著作物であること
  （4）授業の過程における使用を目的とすること
  （5）必要と認められる限度内であること
  （6）著作物の種類・用途、複製の数・態様に照らして著作権者の利益を不当に害しないこと

ディジタル著作権管理
Digital _____ _____ (DRM)

技術	開発	対象	備考
CSS	_____, パナソニック	DVD-Video	アクセス制御技術
AACS	AACS	BD-ROM	
	インテル, IBM, 東芝, パナソニック	DVD-R, RAM, RW, SDメモリー	
B-CAS	パナソニック	地上波ディジタル	機器認証
FairPlay	Apple	iPod, iPhone	

ダビング10

- 2008年7月4日運用開始
  - ディジタル放送の私的利用規定
  - 従来:　　ムーブ1回
  - ダビング10:　コピー9回＋ムーブ1回



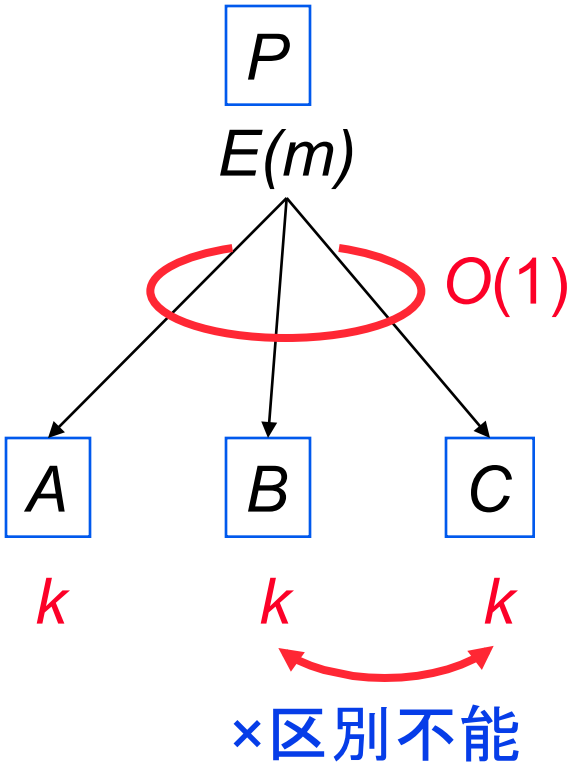
http://panasonic.jp/diga/info/index.html

著作権保護対策

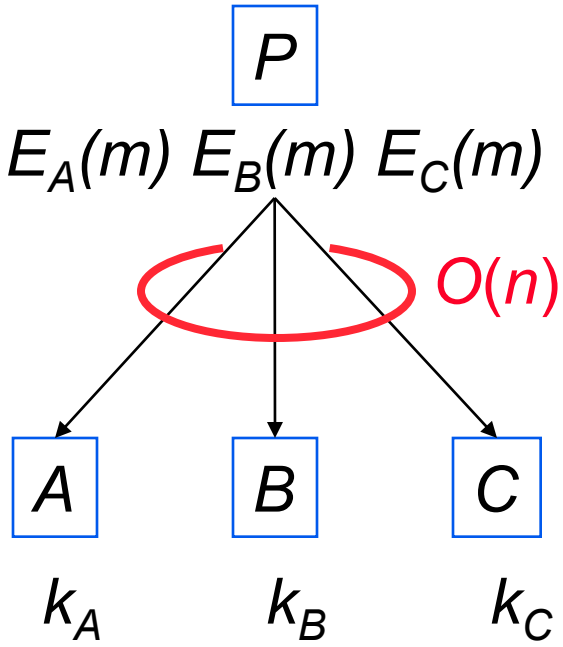
- 1. 専用アプリ
  - ipat, kindle, ebi-reader
- 2. コピー制御技術
  - CPRM
- 3. 情報ハイディング
  - 電子_____

ナイーブな2方式

- 共通鍵



- 個別鍵

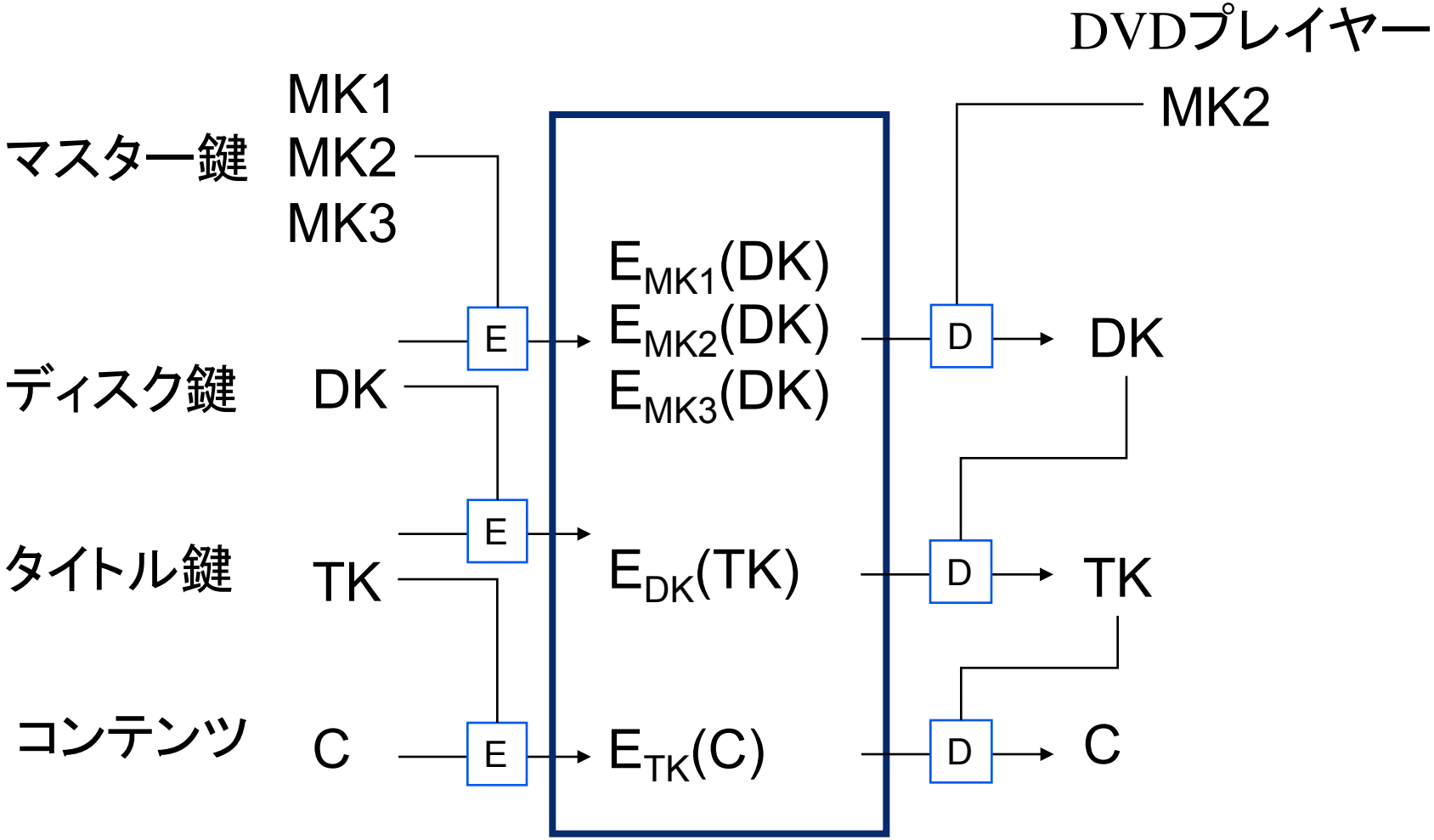


× 個別配信コスト

CPPM/CPRM

- Content Protection for Prerecorded Media/CPRM（_____ Protection for _____ Media）
  - DVDのコピー制御技術
  - プレイヤー: デバイス鍵
  - DVD: メディア鍵

CSS (Content Scrambling System)

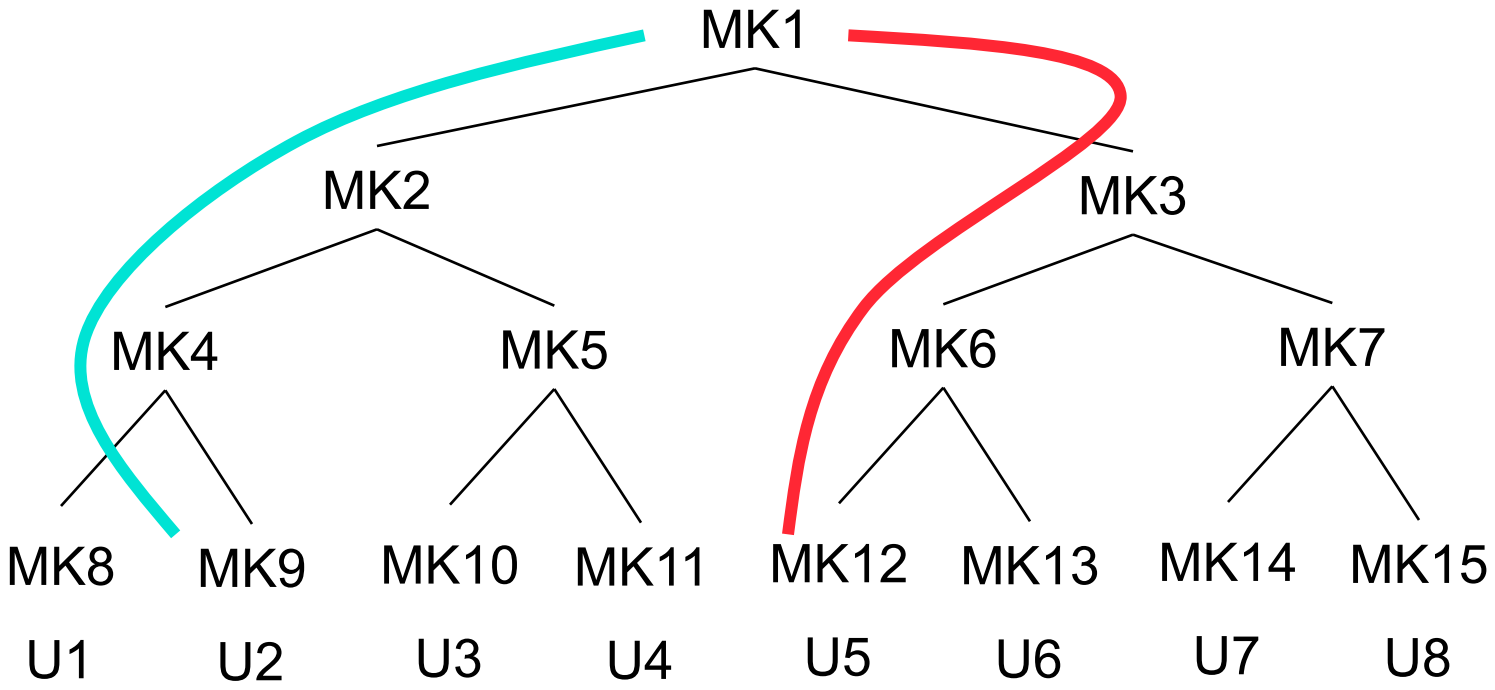


放送暗号の原理

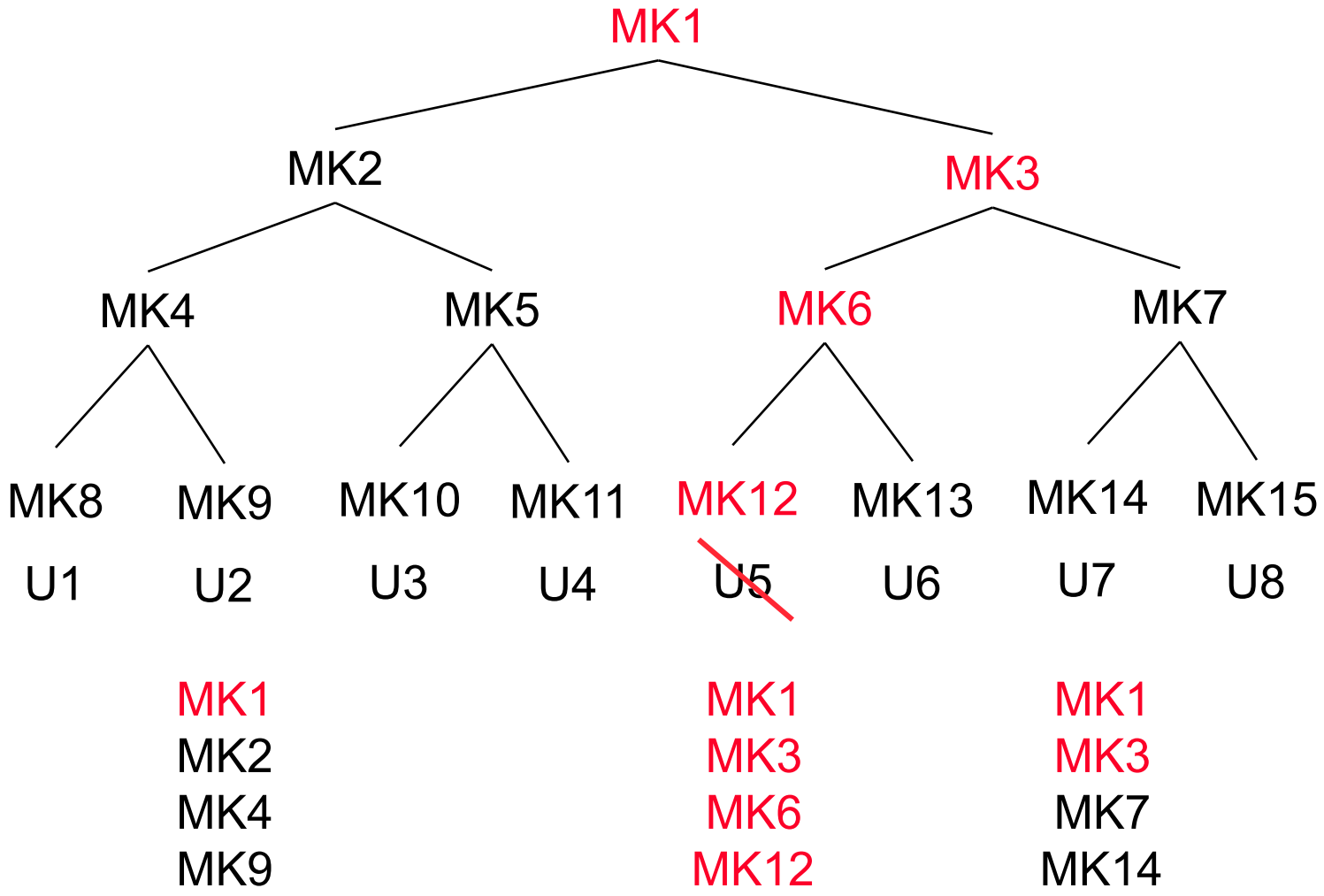
- アイデア
  - 各ユーザ(プレイヤー)に複数の鍵を配布.

U1	U2	U3	
MK1		MK1	
MK2	MK2		
	MK3	MK3	
X	○	○	MK3で暗号化
			MK1で暗号化
X	X	○	?

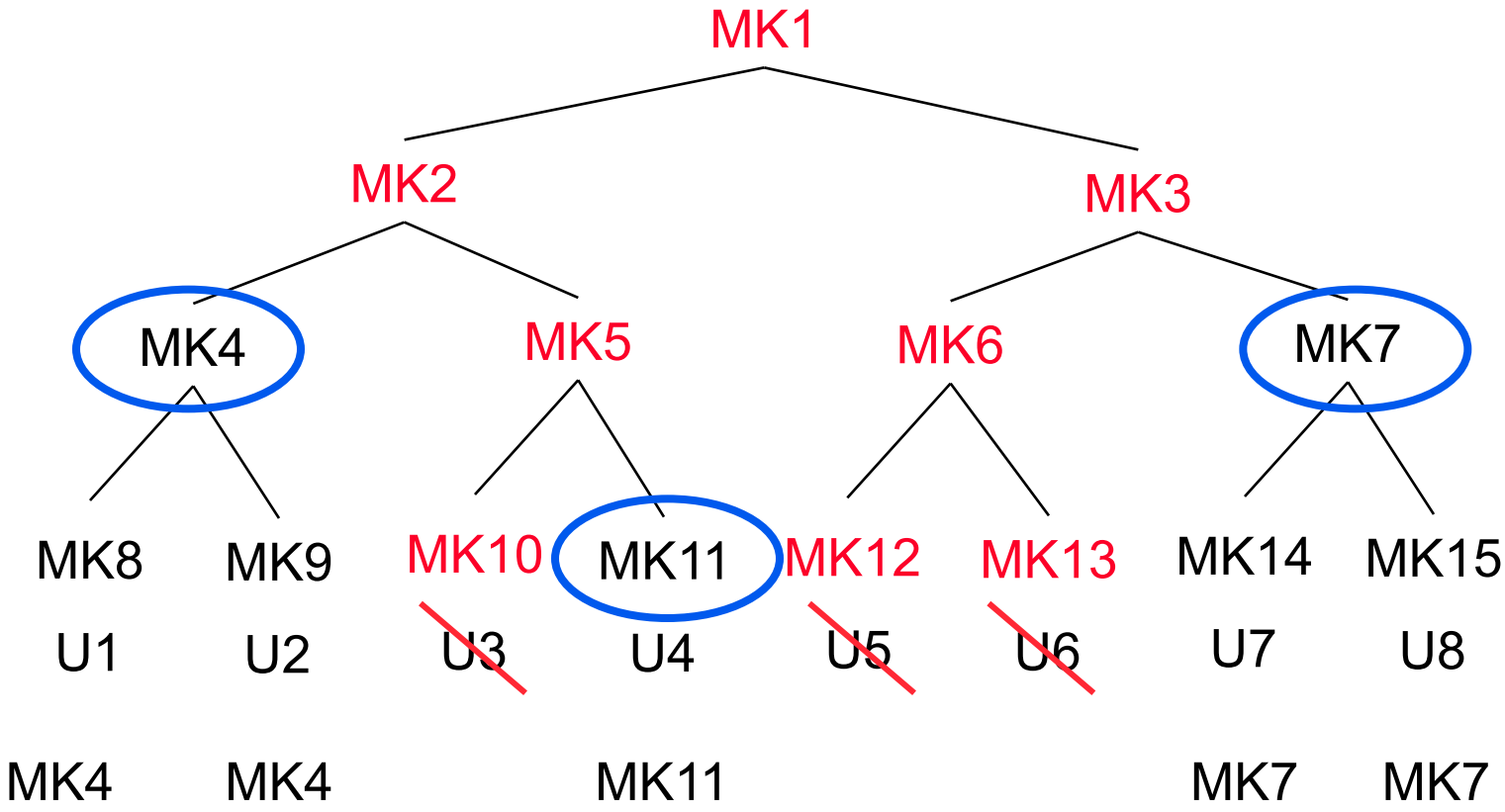
LKH (Logical Key)



2. U5の失効


MK1
MK2
MK3
MK4
MK5
MK6
MK7
MK8
MK9
MK10
MK11
MK12
MK13
MK14
MK15
U1
U2
U3
U4
U5
U6
U7
U8
MK1
MK2
MK4
MK9
MK1
MK3
MK6
MK12
MK1
MK3
MK7
MK14

3. R={U3, U5, U6}の＿＿＿＿



鍵集合　S = {MK4,　　,　　}

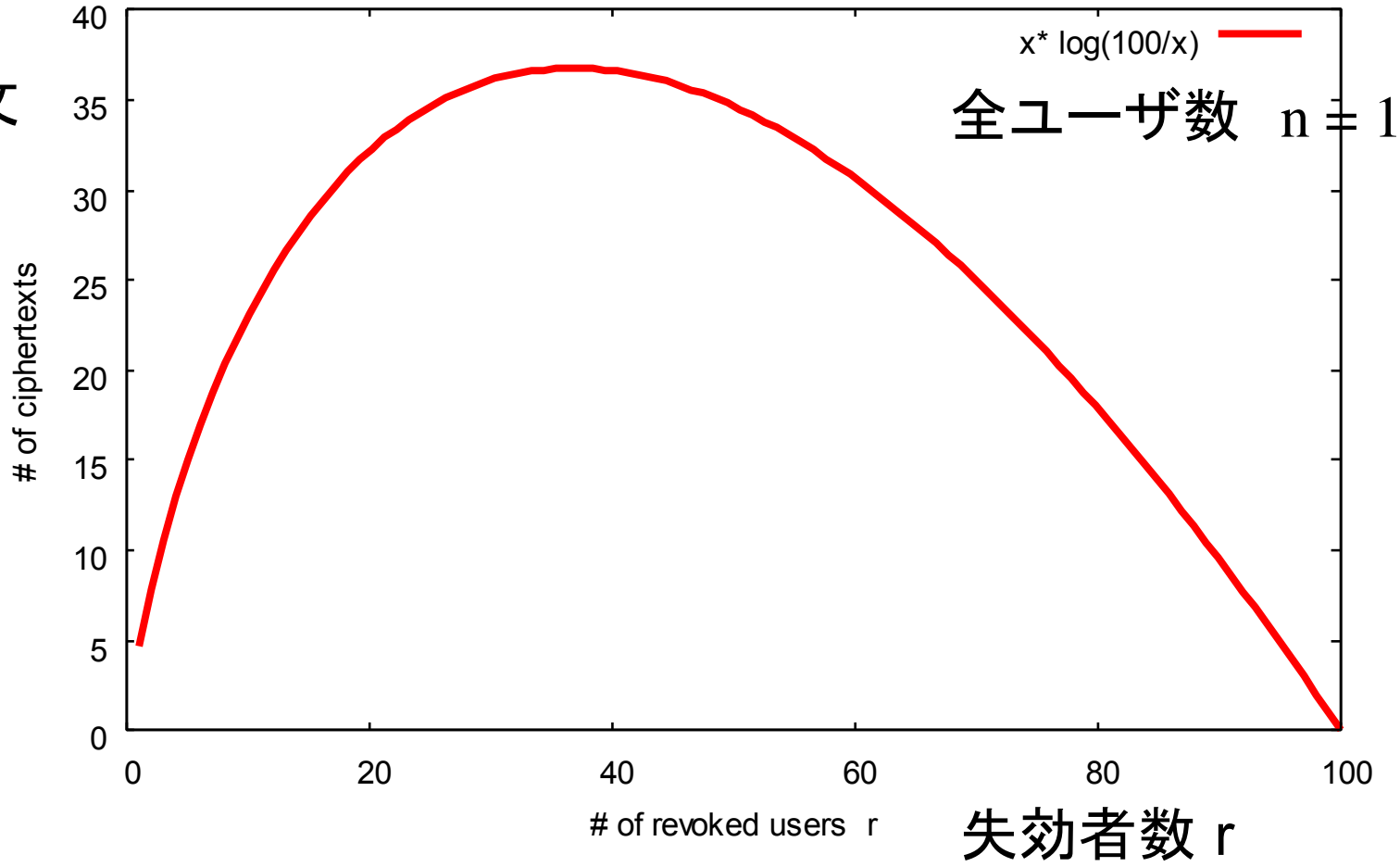
ディスク鍵　$E_4(DK)$, $E_{11}(DK)$, $E_7(DK)$

管理する鍵の数

- ユーザ数 n = 8
- 木の高さ h = 3
  - $n = 2^h$
  - $\log_2 (n) = h$
  - 管理する鍵数: h+1 = 4 [個/ユーザ]
- 失効者数r
  - r=0 の時，暗号文 $E_{MK1}(DK)$　　1個
  - r=1 の時，暗号文 $E_{MK2}(DK)$, $E_{MK7}(DK)$　　個
  - rの時，？

暗号化コスト(暗号化回数)

暗号文数



まとめ

- DVDなどをコピーするのは（　　）の範囲内で許されている.
- CSS, CPRMなどの暗号化によるコピー制御の技術を（　　）という.
- CSSは，全DVDプレイヤーについての（　　）鍵でディスク鍵を暗号化する.
- LKHは木構造でデバイス鍵を管理し，不正なデバイスを（　　）する. これを（　　）暗号という.

演習

- ユーザ数 n = 8のLKHを考えよ.
  - U_4が管理する全てのマスター鍵を求めよ.
  - R={U_2, U_4}を失効するとき，ディスク鍵の暗号化に使う鍵集合K_1を求めよ.
  - R={U_2, U_3, U_4, U_7}が失効した時の鍵集合K_2を求めよ.
  - ユーザ数n = 1024の時，各ユーザが管理するマスター鍵の総数を求めよ.
  - その時，U_2が失効した．鍵集合K_3を求めよ.